DLA PIPER US LLP
ROY K. MCDONALD, Bar No. 193691
roy.mcdonald@dlapiper.com
STEPHEN CHIARI, Bar No. 221410
stephen.chiari@dlapiper.com
DAVID M. DOYLE, Bar No. 233439
david.doyle@dlapiper.com
153 Townsend Street, Suite 800
San Francisco, CA 94107-1957
Tel: 415.836.2500
Fax: 415.836.2501

T. WADE WELCH & ASSOCIATES
CHAD M. HAGAN (*pro hac vice*)
chagan@twwlaw.com
CHRISTINE D. WILLETTS (*pro hac vice*)
cwilletts@twwlaw.com
2401 Fountainview, Suite 700
Houston, Texas 77057
Tel: 713.952.4334
Fax: 713.952.4994

Attorneys for Plaintiffs
DISH NETWORK L.L.C., ECHOSTAR
TECHNOLOGIES CORPORATION and
NAGRASTAR L.L.C.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

DISH NETWORK L.L.C., a Colorado Limited Liability Company, ECHOSTAR TECHNOLOGIES L.L.C., a Texas Limited Liability Company, and NAGRASTAR L.L.C., a Colorado Limited Liability Company, Plaintiffs, v. SatFTA aka SERGEI ALEX ALEXEYEV, Defendant.	CASE NO. 08 CV 01561 JF (PVT) **DECLARATION OF RENEE COLTHARP IN SUPPORT OF APPLICATION FOR ORDER FOR PUBLICATION OF SUMMONS AND TO EXTEND TIME TO EFFECTUATE SERVICE**

I, Renee Coltharp, declare:

1. I am a Senior Staff Auditor II and Fraud Investigator for Plaintiff DISH NETWORK L.L.C. in this action. I have personal knowledge of the facts contained in this declaration and if called as a witness could and would testify thereto.

2. This declaration is being submitted in support of Plaintiffs DISH Network L.L.C., EchoStar Technologies L.L.C. and NagraStar LLC's (collectively "Plaintiffs" or "EchoStar") application for an order directing publication of summons against Defendant SatFTA aka SERGEI ALEX ALEXEYEV ("Defendant") pursuant to the provisions of California Code of Civil Procedure section 415.50.

3. DISH Network is a multi-channel video provider, providing video, audio, and data services to customers throughout the United States, Puerto Rico, and the U.S. Virgin Islands via a Direct Broadcast Satellite ("DBS") system. DISH Network uses high-powered satellites to broadcast, among other things, movies, sports, and general entertainment services ("Programming") to consumers who have been authorized to receive such services after payment of a subscription fee (or in the case of a pay-per-view movie or event, the purchase price).

4. At various times during the 2001-2006 timeframe, Defendant developed and publicly distributed certain piracy codes and software for the purpose of circumventing, and facilitating others in circumventing, Plaintiffs' security system. More specifically, Defendant developed and publicly distributed a piracy file known as IRDr.exe. This program is used to extract proprietary data from Plaintiffs' software contained within the DISH Network receiver or IRD, which can then be used by pirates to program a pirate smartcard device to receive unauthorized programming. There is no reason that any of Plaintiffs' legitimate subscribers would need knowledge of these encryption keys and/or how to extract them from Plaintiffs' IRDs. Defendant's IRDr.exe program also contains a location ID calculator, which assists users in placing multiple receivers on an existing account at a $5 incremental cost instead of a full subscription charge of $25-$100 per account.

5. Defendant also engaged in the development and distribution of a piracy file known as IRDcM.exe. This file provides the ability to determine which channels and tiers are available

on the different satellites used in the DISH Network platform. IRDcM.exe works by examining proprietary data in the satellite receiver and, by assisting pirates in gaining unauthorized access to the table contained in the IRD's RAM, so that they can update, modify and/or re-program their illegal smartcards to circumvent Plaintiffs' ECMs launched to disable the very devices that Defendant's program allows them to reprogram. There is no legitimate purpose for an authorized DISH Network subscriber to have access to this information – which is used by pirates solely for the purpose of stealing Plaintiffs' encrypted programming.

6. Defendant also developed and distributed a piracy diagram known as i2c.jpg. This diagram details the electrical circuitry for interfacing to the memory of a DISH Network IRD and assists pirates in building pirate devices that are unaffected by the electronic counter measures ("ECMs") implemented by Plaintiffs to protect their signal from unauthorized reception and decryption.

7. Defendant also developed and distributed a piracy diagram called jm.gif. This diagram discloses proprietary information relating to the layout of Plaintiffs' security software. JM.gif details the exact location of critical data secured within Plaintiffs' IRD memory, including the memory location of various encryption and cryptographic keys used to secure communications between Plaintiffs' IRD and smartcards.

8. Defendant also developed and distributed a piracy file known as jtag-pcb2.bmp. This file discloses proprietary information about the layout of Plaintiffs' hardware and details the circuitry layout required to interface with the software of Plaintiffs' IRDs. With this diagram pirates can build a device to interface with Plaintiffs' software and allow them to download that software (as well as uploading new versions of that software) for use in circumventing ECMs launched by Plaintiffs to disable pirate devices.

9. In addition to the foregoing, I am informed and believe that Defendant developed and distributed, and/or assisted in the development and distribution of, the following piracy-related files: list501-4sectors.c, bind522, DNLview, getfw, getSDT, info.c, stc721.c, BindKeyMaker, csum, DE, DNLlist, FindR00, GetTable, IRDcm, LSPC, ParseEMMstream, PVRdFormat, PVRExplorer, TSRPP, CnTrList, DishUpgrade, DishVuEPG, FlashEdit, 12Clog,

IDread, jtag_r, jtag_2, mEEP.

10. Defendant distributed the aforementioned piracy codes and software on various hacker websites including: www.innermatrix.com (and innermatrix chat forum); www.interestingDevices.com (and interesting devices chat forum). Defendant published these piracy codes and software to facilitate and/or otherwise assist others in the circumvention of Plaintiffs' security system and the unauthorized reception and decryption of Plaintiffs' copyrighted programming. Defendant's piracy codes and software was downloaded hundreds of times for use by EchoStar pirates.

11. On March 31, 2006, United States federal agents executed a raid and search warrant at Defendant's residence. During the raid the agents seized, among other items, 9 computer hard drives, 12 EchoStar smartcards and 20 EchoStar IRDs (satellite receivers). The FBI and United States Attorneys Office provided Plaintiff s with an opportunity to inspect and analyze the seized materials through proper chain-of-custody requests. Based on that analysis, Plaintiffs discovered the following:

a. 13 of the EchoStar IRDs contained patent modifications including, *inter alia*, unauthorized pins mounted to the circuitry boards, and unauthorized cables and/or wires soldered to contacts contained in the circuitry boards. Four of these IRDs also contained coding in the non-volatile memory that was left as a result of the units being "hit" by one of Plaintiffs' ECMs which targeted illegally modified receivers. Seven of the IRDs also contained additional evidence of unauthorized modifications including holes drilled into the chassis and damage done to the JTAG contacts of the receivers;

b. 4 additional EchoStar receivers were seized which contained unauthorized software modifications including modifications to the cryptography keys, boot software and main software which allow the receivers to circumvent EchoStar's security system and gain access to programming that the receivers were not authorized to receive. One of these IRDs (R0028552448) was modified to match the boot software of another EchoStar receiver thereby creating an unauthorized "clone" which was capable of receiving all of the information, data and programming which was sent to, or authorized to be received by, the original receiver.

programming which was sent to, or authorized to be received by, the original receiver.

12. Defendant was also observed (and admitted to) using illegally modified EchoStar IRDs and smartcards to circumvent Plaintiffs' security system and steal the copyrighted DISH Network programming.

I declare under penalty of perjury under the laws of the United States of America and of the State of California that the foregoing is true and correct. Executed this 27 day of June 2008 at Englewood, Colorado.

Renee Coltharp
Renee Coltharp